



Find: spoofing and ip and mac and arp

Documents

Citations

Searching for **spoofing and ip and mac and arp**.Restrict to: [Header](#) [Title](#) Order by: [Expected citations](#) [Hubs](#) [Usage](#) [Date](#) Try: [Google \(CiteSeer\)](#) [Google \(Web\)](#) [Yahoo!](#) [MSN](#) [CSB](#) [DBLP](#)

5 documents found. Order: number of citations.

[Authenticated Ad Hoc Routing at the Link Layer for Mobile Systems - Binkley, Trost \(1996\)](#) (Correct) (5 citations)

eliminated. Security problems associated with **ARP spoofing** are also reduced. This link-level protocol is Portland State University implementation of Mobile-IP. The routing protocol addresses link security [www.cs.pdx.edu/~jrb/jrb.papers/adhoc2/adhoc2.ps](http://www.cs.pdx.edu/~jrb/jrb.papers/adhoc2/adhoc2.ps)

**One or more of the query terms is very common - only partial results have been returned. Try [Google \(CiteSeer\)](#).**

[Page 1 of 5 - Towards Layer Authentication](#) (Correct)

Attacks based on Address Resolution Protocol **Spoofing** Sean H. Whalen Department of Computer Science, with a mapping between Layer 2 (**MAC**) and Layer 3 (**IP**) addresses. By sending forged **ARP** replies, network clients with a mapping between Layer 2 (**MAC**) and Layer 3 (**IP**) addresses. By sending forged [www.node99.org/projects/l2auth/l2auth.pdf](http://www.node99.org/projects/l2auth/l2auth.pdf)

[Unknown - Guillermo Mario Marro](#) (Correct)

recently incorporated signatures to detect **ARP spoofing** activities which occur at L2, but no other L2 usually operate at layer 3 or above on the TCP/IP stack because layer 2 protocols in local area . 14 4.2.3 More complex state machines . [seclab.cs.ucdavis.edu/papers/Marro\\_masters\\_thesis.pdf](http://seclab.cs.ucdavis.edu/papers/Marro_masters_thesis.pdf)

Try your query at: [Google \(CiteSeer\)](#) [Google \(Web\)](#) [Yahoo!](#) [MSN](#) [CSB](#) [DBLP](#)CiteSeer.IST - Copyright [Penn State](#) and [NEC](#)